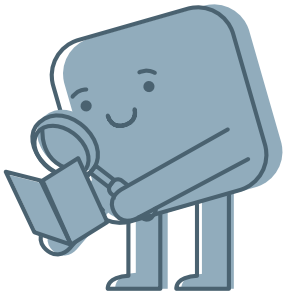
Social Engineering



Social Engineering bedeutet, dass Angreifende versuchen uns als Menschen zu manipulieren, um an Daten und Informationen zu kommen. Dies passiert über verschiedene Kanäle (USB-Sticks, SMS, Anrufe, Phishing, Persönliche Gespräche uvm.)

Die Phasen eines Eingriffs:

1) Ausspionieren (die Angreifer sammeln Informationen, z.B. frei zugängliche über Social Media, Stelleninserate, Website und vieles mehr)
2) Vorbereiten eines Angriffs (mit den gesammelten Informationen wird ein Angriffsplan geschmiedet)
3) Kontakt aufnehmen (per E-Mail, Telefon, SMS oder auch persönlich wird Kontakt aufgenommen)
4) Einnisten (entweder persönlich, wenn man sich dauerhaften Zutritt verschafft hat oder aber über eine schädliche Software, die sich nun im System verbreitet)
5) Eskalation (die Software wird genutzt, um umfangreichere Rechte zu erlangen, bzw. der persönliche Zutritt wird erweitert in dem man in nicht freizugängliche Unternehmensbereiche eindringt)
6) Ausbreitung in der Organisation (mehr und mehr Daten und Informationen werden gesammelt)
7) Diebstahl (in Form von Daten und Informationen, aber auch physisch vor Ort möglich)

Social Engineering passiert nicht nur bei Unternehmen und Organisationen, sondern auch bei Einzelpersonen. Dabei werden unsere menschlichen Eigenschaften, wie zum Beispiel Neugier und Hilfsbereitschaft, aber auch unser Stolz und unsere Bequemlichkeit gerne ausgenutzt.

Folgende Punkte, solltest du berücksichtigen:

1) Überlege genau, welche Inhalte du teilst (z.B. auf Social Media).
2) Teile niemals vertrauliche Informationen deiner Organisation!
3) Teile niemals deine Passwörter, Zugangsdaten oder Kontoinformationen! Die sind nur für dich bestimmt!
4) Bei vertraulichen Inhalten in Telefonaten oder Gesprächen: Achte auf deine Umgebung! Wer hört mit?
5) Vertrauen ist gut, Kontrolle ist besser! Unbekannter Anrufer? Versuche den Anrufer zu identifizieren. Wenn du dir unsicher bist, rufe eine dir bekannte Nummer zurück!
6) Achte bei E-Mails auf den Absender. Folge Forderungen von Banken, Paketdiensten oder auch anderen Absendern nicht blind. Prüfe immer, ob es sich um eine Phishing-E-Mail handelt.
7) Du bist nicht allein! Melde verdächtige Vorfälle in deiner Organisation an die zuständige Stelle. Im privaten Umfeld melde verdächtige Situationen an die Polizei!
8) Überweise niemals Geld an unbekannte Personen. Händige ebenso kein Geld oder Wertsachen an vermeintliche Polizisten aus.

Verdächtige Vorfälle melde umgehend in deiner Organisation oder im privaten Umfeld an die Polizei!

DACHVERBAND
WIENER SOZIALEINRICHTUNGEN